AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Previously Presented) A method for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, said belief state indicating a state of at least one system resource or service; and

(b) adjusting a prior belief state of the first sensor, said belief state indicating a state of at least one system resource or service, the adjustment based at least in part on the second sensor's belief state.

2. (Original) The method of claim 1 wherein the first and second sensors are different types of sensors.

3. (Original) The method of claim 2 wherein the first sensor is a probabilistic sensor.

4. (Original) A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a monitored resource; and

(b) adjusting a prior belief state of the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm.

5. (Original) A method for enhancing the sensitivity of an intrusion detection system

that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on monitored computer system resources; and

(b) adjusting a prior belief state of the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious.

6. (Previously Presented) A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) identifying a set of potentially similar features shared by a new alert and one or more existing alert classes;

(b) comparing the new alert to one or more existing alert classes;

(c) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(d1) associating the new alert with the existing alert class that the new alert most closely matches; or

(d2) defining a new alert class that is associated with the new alert.

7. (Original) A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) receiving a new alert;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) updating a similarity expectation for one or more feature values;

(d) comparing the new alert with one or more alert classes, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert.

8. (Original) The method of claim 7 further comprising the step (a1) of passing each existing alert class through a transition model to generate a new prior belief state for each alert class.

9. (Original) A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding features;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert.